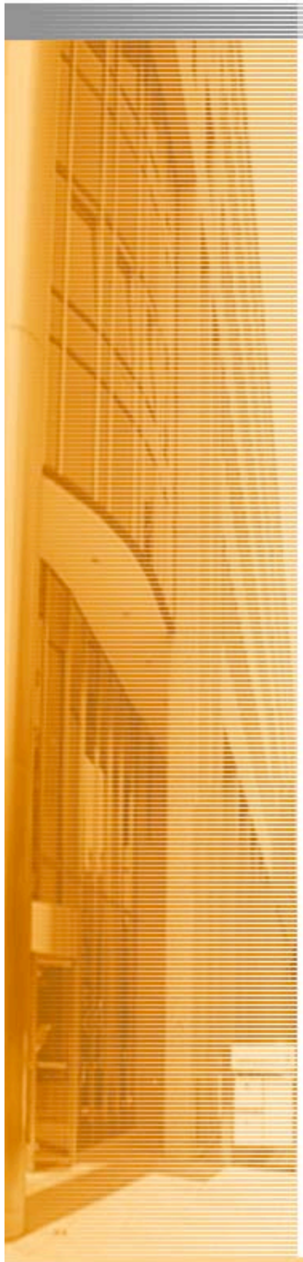
Fraunhofer Institute for Open Communication Systems

Privacy in the Network on Wheels Project

SEVECOM Workshop, 1. -2. Feb 2006

matthias.gerlach@fokus.fraunhofer.de

Privacy Definitions (1)



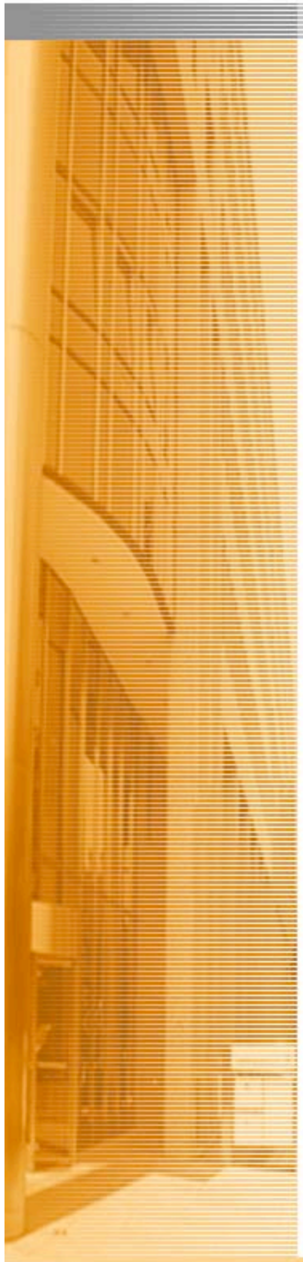
Privacy

- The “interest that individuals have in sustaining a 'personal space', free from interference by other people and organizations” [Clarke97]
- The “right to be left alone - the most comprehensive of rights, and the right most valued by free people” [Louis Brandeis 1890]
- Different dimensions:
  - physical (physical integrity of the individual)
  - behavior (political, sexual behavior not disclosed)
  - information privacy
    - personal communications (communication is not monitored)
    - personal data (user can control dissemination of own data)

And In the Context of Communication?

- The information that are disclosed by the communication system.
  - location, speed, purchases, connections to others, information retrieved, ...
- Users may want to control the dissemination of those information.

Privacy Definitions (2) [Pfitzmann00]



Anonymity

- "Anonymity is the state of being not identifiable within a set of subjects, the anonymity set. "

Pseudonymity

- "Pseudonymity is the use of pseudonyms as identifiers."

Unlinkability

- The probability of two items being related stays the same before and after a run of the system.

Unobservability

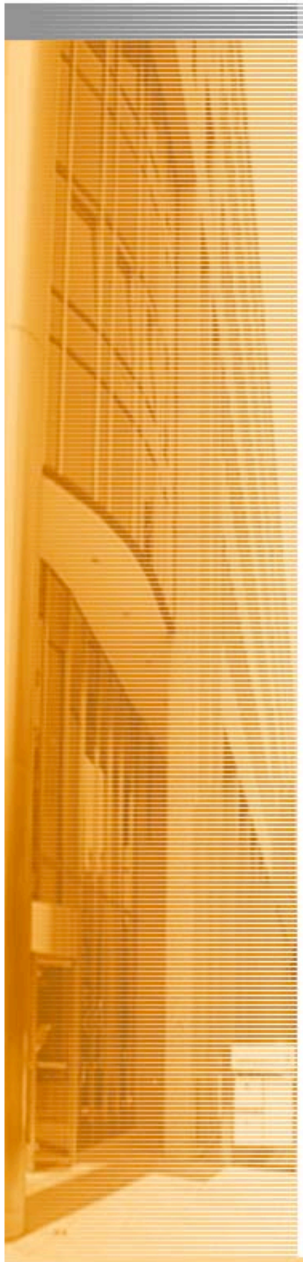
- "Unobservability is the state of IOIs being indistinguishable from any IOI at all. "

Location Privacy

- "The ability to prevent others from learing one's current or past location" [Beresford03]

IOI - Item of Interest

Attacker Models (1)



All-Knowing Attacker

- Owns a global grid of receivers with a certain density
- Networked grid of receivers
- Receivers may also provide useful services (LBA)

Attacker with local connectivity

- Owns a Transceiver (and can issue messages)
- Legitimate Part of the Network

Attacker today

- Sits in a car and follows you
- Police: ask many police officers to watch out for a specific vehicle
- Installs many cameras registering Number-Plates

Attacker Models (2)

Attackers could be

- Big Brother Governments
- Insurance companies
- Curious Individuals
- Jealous (Girl-/Boy-) Friends
- Private Investigators
- Terrorists
- The Press

There are (even legitimate) reasons to diminish privacy!

These have to be examined on a per application basis

Attacks on Privacy discussed up to now

Focus on the globally networked attacker

- The hardest attacker model
- Yet not the most improbable
- Think of
  - Petrol Stations
  - The many existing WiFi access points in cities
  - VII installing many roadside units

Attacks on Information Privacy

- Attacker must be networked
- Attacker may use any identifier that is used in the network or the applications
- Attacker may (probably) also correlate other information sources.

Focus up to Now

We acknowledge privacy as an important asset!

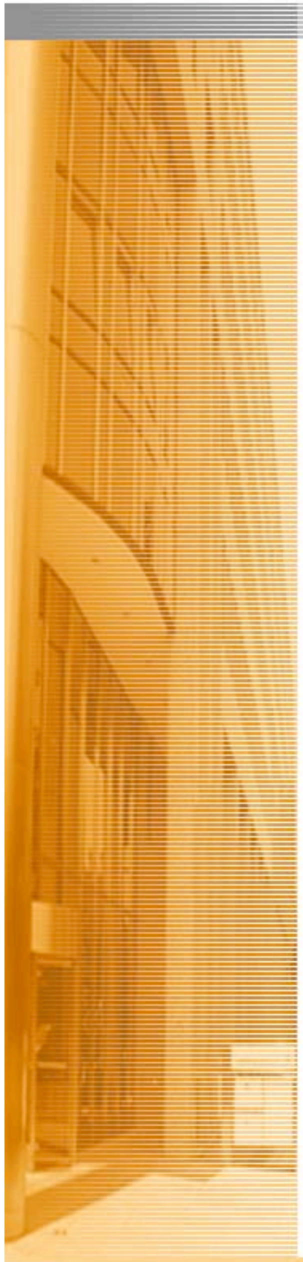
Location Privacy

- As a subclass of Information privacy
- Main attack: trace a node‘s location
- Need any identifier of the node to do this.

Solution

- Changing pseudonyms for the whole communication system
- Trade-off with functionality of the communication system (esp. routing)

Problems with Pseudonyms



Useless in Low Penetration Scenarios

- Anonymity Set Size = 1 implies no anonymity
- Impact on communication system?

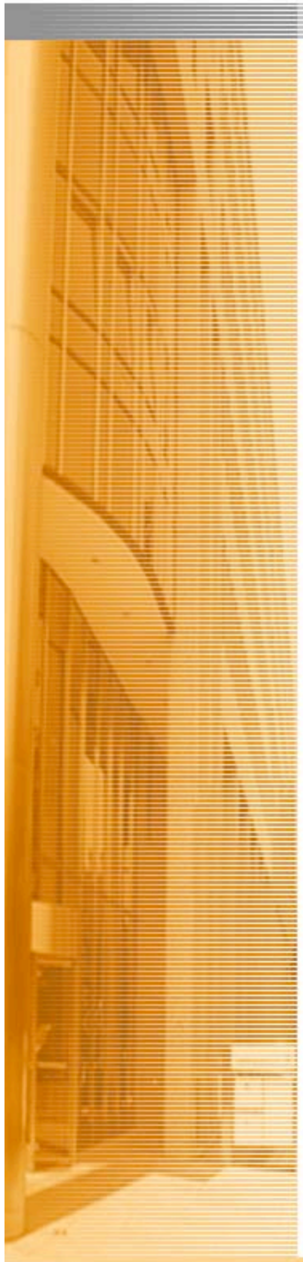
Useless if not changed properly

- Must keep anonymity set large
- Possible correlation by
  - speed
  - lane
  - beacon send frequency
  - direction

Impact on Functionality of Applications / Routing

- Changing a pseudonym means losing connection

Future Work



Examine impact of changing pseudonyms on Routing

- Broken connections (?)
- More management overhead (?)

Look at impact of applications on privacy

- Some Applications only work if there is no (location) privacy

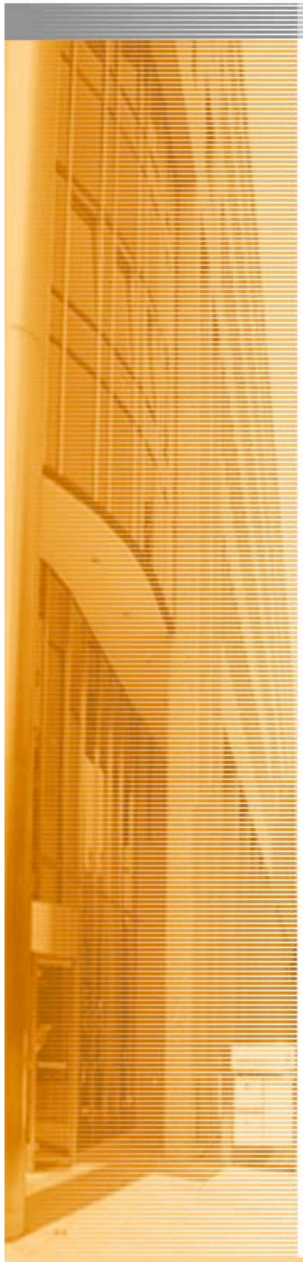
Devise good pseudonym change algorithms

- make anonymity set as large as possible
- create distributed algorithms

Check if existing infos may make pseudonyms obsolete

- e.g. Grid of networked cameras
- mobile phones‘ traceability

Thank you!



Do you have any Questions?

References

- [Clarke97] R. Clarke. Privacy and dataveillance, and organisational strategy. http://www.anu.edu.au/people/Roger.Clarke/DV/PStrat.html.
- [Pfitzmann00] A. Pfitzmann and M. Köhntopp. Anonymity, unobservability, and pseudonymity - a proposal for terminology. In Designing Privacy Enhancing Technologies: International Workshop on Design Issues in Anonymity and Unobservability, 2000.
- [Beresford03] A. R. Beresford and F. Stajano. Location privacy in pervasive computing. IEEE Pervasive Computing, pages 46-55, 2003.
- www.network-on-wheels.de